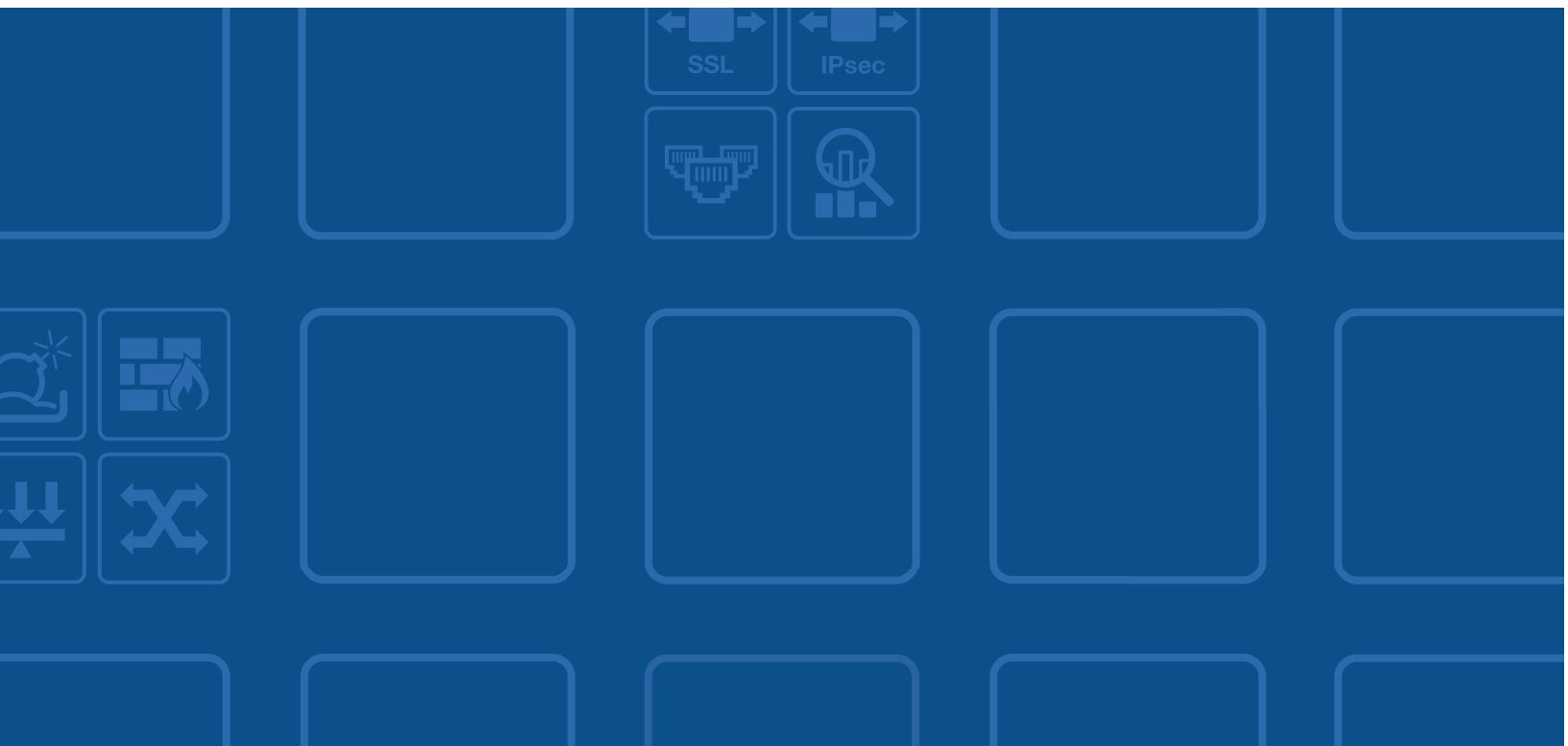
FORTINET
High Performance Network Security

# FortiOS - Release Notes

VERSION 5.4.0



**FORTINET DOCUMENT LIBRARY**

http://docs.fortinet.com

**FORTINET VIDEO GUIDE**

http://video.fortinet.com

**FORTINET BLOG**

https://blog.fortinet.com

**CUSTOMER SERVICE & SUPPORT**

https://support.fortinet.com

**FORTIGATE COOKBOOK**

http://cookbook.fortinet.com

**FORTINET TRAINING SERVICES**

http://www.fortinet.com/training

**FORTIGUARD CENTER**

http://www.fortiguard.com

**END USER LICENSE AGREEMENT**

http://www.fortinet.com/doc/legal/EULA.pdf

**FEEDBACK**

Email: techdocs@fortinet.com

January 16, 2018

FortiOS 5.4.0 Release Notes

01-540-293566-20180116

# TABLE OF CONTENTS

# Change Log

| Date | Change Description |
|---|---|
| 2015-12-21 | Initial release. |
| 2015-12-22 | Added, FG-30E, FG50E, FG-51E, FWF-30E, FWF-50E, and FWF-51E to Supported Models. |
| 2015-12-23 | Added FortiAnalyzer and FortiManager 5.4.0 to Product Integration and Support. |
| 2016-01-05 | Added bug 304802 to Known Issues List.<br><br>Added Windows Server 2008 (32-bit and 64-bit) and Novell eDirectory 8.8 to *Product Integration and Support* > *FSSO* section. |
| 2016-01-07 | Changed FortiExplorer support: 2.6 build 1083. |
| 2016-01-11 | Updated Product Integration and Support:<br>FortiSwitch: 3.3.2 and later and supported models. |
| 2016-01-12 | Added 306277, 303661, 305058, and 283697 to Known Issues. |
| 2016-01-27 | Added FortiOS 5.4 Supported Upgrade Path note to Upgrade Information |
| 2016-01-29 | Updated FortiClient iOS support to 5.2.3 and later. |
| 2016-02-16 | Updated *Special Notices* > *FortiAnalyzer Support* section. |
| 2016-02-17 | Updated *Special Notices* > *Log Disk Usage* section. |
| 2016-02-22 | Updated FG-30E, FG50E, FG-51E, FWF-30E, FWF-50E, and FWF-51E to build number 5211, branch point 1011. |
| 2016-03-02 | Updated FG-30E, FG50E, FG-51E, FWF-30E, FWF-50E, and FWF-51E to build number 5227, branch point 1011. |
| 2016-03-04 | Added RHEL 7.1/Ubuntu 12.04 and later to Product Integration and Support. |
| 2016-03-24 | Added FG-30E-MI, FG-30E-MN, FGR-30D, FGR-30D-A, FGR-35D, FWF-30E-MI, and FWF-30E-MN to Support Models. |
| 2016-04-26 | Added FG-3000D to Supported Models. |
| 2016-06-02 | Added Microsoft Windows 10 to SSL VPN support. |
| 2016-06-15 | Added *Model 60D Boot Issue* section to Upgrade Information. |

| Date | Change Description |
|---|---|
| 2016-07-05 | Updated Product Integration and Support information. |
| 2016-07-13 | Updated FG-30E, FG-50E, FG-51E, FWF-30E, FWF-50E, FWF-51E build to 5351.<br>Updated FG-30E-MI, FG-30E-MN build to 5415.<br>Updated FWF-30E-MI, FG-30E-MN build to 5427.<br>Added 274252 to Resolved Issues.<br>Added FG-52E, FG-60E, FG 61E, FG-2000E, FG-2500E, FG-3800D, FWF-60E, and FWF-61E to Supported Models. |
| 2016-07-14 | Added FG-3000D to Supported Models. |
| 2016-09-26 | Added special notice about FortiGate/FortiWiFi 80C and 81CM support. |
| 2016-11-01 | Added *Special Notices > FG-30E-3G4G and FWF-30E-3G4G MODEM Firmware Upgrade* section. |
| 2017-01-25 | Added 289491 to *Known Issues > Upgrade* section. |
| 2017-02-16 | Updated *Special Notices > FortiGate units managed by FortiManager 5.0 or 5.2*. |
| 2017-07-21 | Clarified that you reformat the logdisk after downgrading FortiOS from 5.4 to 5.2. |
| 2017-11-10 | Added 273973 to *Known Issues > Upgrade*. |
| 2018-01-16 | Added *Upgrade Information > Firewall Policies with Wildcard FQDNs are Deleted*. |

# Introduction

This document provides the following information for FortiOS 5.4.0 build 1011:

- Special Notices
- Upgrade Information
- Product Integration and Support
- Resolved Issues
- Known Issues
- Limitations

See the Fortinet Document Library for FortiOS documentation.

## Supported models

FortiOS 5.4.0 supports the following models.

| | |
|---|---|
| **FortiGate** | FG-30D, FG-30E, FG-30E-MI, FG-30E-MN, FG-30D-POE, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-61E, FG-70D, FG-70D-POE, FG-80D, FG-90D, FGT-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-140D, FG-140D-POE, FG- 200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300D, FG-400D, FG-500D, FG-600C, FG-600D, FG-800C, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3800D, FG-3810D, FG-5001C, FG-5001D |
| **FortiWiFi** | FWF-30D, FWF-30E, FWF-30E-MI, FWF-30E-MN, FWF-30D-POE, FWF-50E, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-61E, FWF-90D, FWF-90D-POE, FWF-92D |
| **FortiGate Rugged** | FGR-30D, FGR-30D-A, FGR-35D, FGR-90D |
| **FortiGate VM** | FG-VM32, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN , FG-VMX, |
| **FortiOS Carrier** | FortiOS Carrier 5.4.0 images are delivered upon request and are not available on the customer support firmware download page. |

The following models are released on a special branch based off of FortiOS 5.4.0. As such, the *System > Dashboard > Status* page and the output from the `get system status` CLI command displays the build number.

| | |
|---|---|
| **FG-30E** | is released on build 5351. |
| **FG-30E-MI** | is released on build 5415. |
| **FG-30E-MN** | is released on build 5415. |
| **FG-50E** | is released on build 5351. |
| **FG-51E** | is released on build 5351. |
| **FG-52E** | is released on build 5315. |
| **FG-60E** | is released on build 5335. |
| **FG-61E** | is released on build 5335. |
| **FG-2000E** | is released on build 5391. |
| **FG-2500E** | is released on build 5391. |
| **FG-3000D** | is released on build 7184. |
| **FG-3800D** | is released on build 5472. |
| **FGR-30D** | is released on build 5258. |
| **FGR-30D-A** | is released on build 5258. |
| **FGR-35D** | is released on build 5258. |
| **FWF-30E** | is released on build 5351. |
| **FWF-30E-MI** | is released on build 5427. |
| **FWF-30E-MN** | is released on build 5427. |
| **FWF-50E** | is released on build 5351. |
| **FWF-51E** | is released on build 5351. |
| **FWF-60E** | is released on build 5404. |
| **FWF-61E** | is released on build 5404. |

To confirm that you are running the proper build, the output from the `get system status` CLI command has a **branch point field** that should read 1011.

# What's new in FortiOS 5.4.0

For a list of new features and enhancements that have been made in FortiOS 5.4.0 see the *What's New for FortiOS* 5.4.0 document available in the Fortinet Document Library.

# Special Notices

## FortiGate/FortiWiFi 80C and 81CM Support

FortiOS 5.4.0 does not support FortiGate/FortiWifi 80C and 81CM models. However, support for these models has been added to FortiOS 5.4.1. For information about the supported upgrade paths for these models, see the *Supported Upgrade Paths - FortiOS* at http://cookbook.fortinet.com/sysadmins-notebook/supported-upgrade-paths-fortios/.

## Built-In Certificate

FortiGate and FortiWiFi D-series and above have a built in Fortinet_Factory certificate that uses a 2048-bit certificate with the 14 DH group.

## Default log Setting Change

For FG-5000 blades, log disk is disabled by default. It can only be enabled via CLI. For all 2U & 3U models (FG-3600/FG-3700/FG-3800), log disk is also disabled by default. For all 1U models and desktop models that supports SATA disk, log disk is enabled by default.

## FortiAnalyzer Support

In version 5.4, encrypting logs between FortiGate and FortiAnalyzer is handled via SSL encryption. The IPSEC option is no longer available and users should reconfigure in GUI or CLI to select the SSL encryption option as needed.

## FG-92D High Availability in Interface Mode

The FortiGate-92D may fail to form a HA cluster and may experience a spanning tree loop if it is configured with the following:

- operating in interface mode
- at least one of the interfaces, for example *interface9*, is used has the HA heartbeat interface
- a second interface is connected to an external switch

Workaround: use either WAN1 or WAN2 as the HA heartbeat device.

## FG-900D and FG-1000D

CAPWAP traffic will not offload if the ingress and egress traffic ports are on different NP6 chips. It will only offload if both ingress and egress ports belong to the same NP6 chip.

## FG-3700DX

CAPWAP Tunnel over the GRE tunnel (CAPWAP + TP2 card) is not supported.

## FortiGate units managed by FortiManager 5.0 or 5.2

Any FortiGate unit managed by FortiManager 5.0.0 or 5.2.0 may report installation failures on newly created VDOMs, or after a factory reset of the FortiGate unit even after a retrieve and re-import policy.

## FortiGate-VM 5.4 for VMware ESXi

Upon upgrading to FortiOS 5.4.0, FortiGate-VM v5.4 for VMware ESXi (all models), no longer supports the VMXNET2 vNIC driver.

## FortiPresence

For FortiPresence users, it is recommended to change the FortiGate web administration TLS version in order to allow the connection.

```
config system global
   set admin-https-ssl-versions tlsv1-0 tlsv1-1 tlsv1-2
end
```

## Log Disk Usage

Users are able to toggle disk usage between Logging and WAN Optimization for single disk FortiGates.

To view a list of supported FortiGate models, refer to the FortiOS 5.4.0 Feature Platform Matrix.

## SSLVPN

The following RDP/VNC web portals are not supported for the following platforms:

- FGT-80D
- FGR-90D
- FGT-92D
- FWF-92D
- FGT-200D
- FGT-200D-POE
- FGT-240D
- FGT-240D-POE
- FGT-600C
- FGT-800C
- FGT-1000C
- FGT-3240C
- FGT-3600C
- FGT-5001C

## SSLVPN setting page

The default server certificate has been changed to the `Fortinet_Factory` option. This excludes FortiGate-VMs which remain at the `self-signed` option. For details on importing a CA signed certificate, please see the How to purchase and import a signed SSL certificate document.

## FG-30E-3G4G and FWF-30E-3G4G MODEM Firmware Upgrade

The 3G4G MODEM firmware on the FG-30E-3G4G and FWF-30E-3G4G models may require updating. Upgrade instructions and the MODEM firmware have been uploaded to the Fortinet Customer Support site in the download directory under:

*.../FortiGate/v5.00/5.4/Sierra-Wireless-3G4G-MODEM-Upgrade/*

# Upgrade Information

## Upgrading from FortiOS 5.2.4 or later

FortiOS version 5.4.0 officially supports upgrade from version 5.2.4 or later.

When upgrading from a firmware version beyond those mentioned in the Release Notes, a recommended guide for navigating the upgrade path can be found on the Fortinet documentation site.

There is separate version of the guide describing the safest upgrade path to the latest patch of each of the supported versions of the firmware. To upgrade to this build, go to FortiOS 5.4 Supported Upgrade Paths

## Firewall Policies with Wildcard FQDNs are Deleted

Firewall policies cannot contain wildcard FQDNs. Firewall rules that use wildcard FQDNs are deleted when you upgrade from 5.2.x to 5.4.x. So if you have firewall rules that use wildcard FQDNs, you must reconfigure those rules to remove the wildcards.

## Model 60 D Boot Issue

The following 60D models have an issue upon upgrading to FortiOS 5.4.1. The second disk (flash) is unformatted and results in the /var/log/ directory being mounted to an incorrect partition used exclusively for storing the firmware image and booting.

- FG-60D-POE
- FG-60D
- FWF-60D-POE
- FWF-60D

To fix the problem, follow these steps. If you have not upgraded yet, you only need to perform step 6, otherwise start with step 1.

1. Backup your configuration.
2. Connect to the console port of the FortiGate device.
3. Reboot the system and enter the BIOS menu.
4. Format the boot device.
5. Burn the firmware image to the primary boot device.
6. Once the system finishes rebooting, from the CLI run "execute disk format 16". This will format the second flash disk.
7. Restore your configuration.

## Unified Disk Usage

FortiOS 5.4.0 changes the disk usage behavior upon upgrading from FortiOS 5.2. The table below describes the new logging and WANopt disk usage for single and two disk FortiGate devices running FortiOS 5.4.0.

| | | |
|---|---|---|
| **Single Disk Platforms (Logging or WANopt)** | | |
| | **Only Logging enabled** | No change. |
| | **Only WANopt enabled** | No change. |
| | **Both Logging & WANopt enabled** | In 5.4.0, the upgrade process configures the disk for Logging. However, you may change the disk to use WANopt. |
| **Two Disk Platforms (First disk is reserved for Logging; the second is reserved for WANopt)** | | |
| | **Only Logging enabled on the first disk** | No change. |
| | **Only Logging enabled on the second disk** | In 5.4.0, Logging is changed to the first disk. The Logging data is lost on the second disk. |
| | **Only WANopt enabled on the first disk** | In 5.4.0, WANopt is changed to the second disk. The WANopt cache is lost on the first disk. |
| | **Only WANopt enabled on the second disk** | No change. |
| | **Both Logging & WANopt enabled** | Regardless of the 5.2 configuration, the 5.4.0 upgrade process will change the configuration so that Logging uses the first disk and WANopt uses the second disk.<br><br>Logging data and WANopt cache may or may not be lost depending on which disk they were configured on prior to upgrading. |

## FortiGate-VM 5.4 for VMware ESXi

Upon upgrading to FortiOS 5.4.0, FortiGate-VM v5.4 for VMware ESXi (all models), no longer supports the VMXNET2 vNIC driver.

## Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- VDOM parameters/settings
- admin user account
- session helpers
- system access profiles.

When downgrading from 5.4 to 5.2, users will need to reformat the logdisk after the downgrade.

## FortiGate VM firmware

Fortinet provides FortiGate VM firmware images for the following virtual environments:

**Citrix XenServer and Open Source XenServer**

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the QCOW2 file for Open Source XenServer.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

**Linux KVM**

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains QCOW2 that can be used by `qemu`.

**Microsoft Hyper-V**

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.hyperv.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains three folders that can be imported by Hyper-V Manager on Hyper-V 2012. It also contains the file `fortios.vhd` in the Virtual Hard Disks folder that can be manually added to the Hyper-V Manager.

**VMware ESX and ESXi**

- `.out`: Download either the 32-bit or 64-bit firmware image to upgrade your existing FortiGate VM installation.

- `.ovf.zip`: Download either the 32-bit or 64-bit package for a new FortiGate VM installation. This package contains Open Virtualization Format (OVF) files for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

## Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

# Product Integration and Support

## FortiOS 5.4.0 support

The following table lists 5.4.0 product integration and support information:

| | |
|---|---|
| **Web Browsers** | • Microsoft Internet Explorer version 11<br>• Mozilla Firefox version 37<br>• Google Chrome version 43<br>• Apple Safari version 7.0 (For Mac OS X)<br>Other web browsers may function correctly, but are not supported by Fortinet. |
| **Explicit Web Proxy Browser** | • Microsoft Internet Explorer versions 8, 9, 10, and 11<br>• Mozilla Firefox version 27<br>• Apple Safari version 6.0 (For Mac OS X)<br>• Google Chrome version 34<br>Other web browsers may function correctly, but are not supported by Fortinet. |
| **FortiManager** | For the latest information, see the FortiManager and FortiOS Compatibility.<br>You should upgrade your FortiManager prior to upgrading the FortiGate. |
| **FortiAnalyzer** | For the latest information, see the FortiAnalyzer and FortiOS Compatibility.<br>You should upgrade your FortiAnalyzer prior to upgrading the FortiGate. |
| **FortiClient Microsoft Windows and FortiClient Mac OS X** | • 5.2.5 and later |
| **FortiClient iOS** | • 5.2.3 and later |
| **FortiClient Android and FortiClient VPN Android** | • 5.2.6 and later |

| | |
|---|---|
| **FortiAP** | • 5.2.5 and later<br>• 5.0.10<br>You should verify what the current recommended FortiAP version is for your FortiAP prior to upgrading the FortiAP units. You can do this by going to the *WiFi Controller* > *Managed Access Points* > *Managed FortiAP* page in the GUI. Under the *OS Version* column you will see a message reading *A recommended update is available* for any FortiAP that is running an earlier version than what is recommended. |
| **FortiSwitch OS (FortiLink support)** | • 3.3.2 and later<br>Supported models: FS-108D, FS-124D, FS-124D-POE, FS-124D-FPOE, FS-224D-POE, FS-224D-FPOE, FS-248D-POE, FS-248D-FPOE, FS-424D, FS-424D-POE, FS-424D-FPOE, FS-448D, FS-448D-POE, FS-448-FPOE, FS-524D, FS-524-FPOE, FS-548D, FS-548-FPOE, FS-1024D, FS-1048D, FS-3032D, FSR-112D-POE<br>• 3.3.0 and later<br>Supported models: FS-108D-POE, FS-224D-POE, FS-124D, FS-124D-POE, FS-224D-FPOE, FSR-112D-POE<br>• 3.2.0 and later<br>Supported models: FS-108D-POE, FS-224D-POE, FSR-112D-POE<br>• 3.0.1 and later<br>Supported model: FS-224D-POE<br>• 2.0.3<br>Supported models: FS-28C, FS-324B-POE, FS-348B, FS-448B |
| **FortiController** | • 5.2.0 and later<br>Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C<br>• 5.0.3 and later<br>Supported model: FCTL-5103B |
| **FortiSandbox** | • 2.1.0 and later<br>• 1.4.0 and later |

| | |
|---|---|
| **Fortinet Single Sign-On (FSSO)** | • 5.0 build 0242 and later (needed for FSSO agent support OU in group filters)<br>  • Windows Server 2008 (32-bit and 64-bit)<br>  • Windows Server 2008 R2 64-bit<br>  • Windows Server 2012 Standard<br>  • Windows Server 2012 R2 Standard<br>  • Novell eDirectory 8.8<br>• 4.3 build 0164 (contact Support for download)<br>  • Windows Server 2003 R2 (32-bit and 64-bit)<br>  • Windows Server 2008 (32-bit and 64-bit)<br>  • Windows Server 2008 R2 64-bit<br>  • Windows Server 2012 Standard Edition<br>  • Windows Server 2012 R2<br>  • Novell eDirectory 8.8<br>FSSO does not currently support IPv6. |
| **FortiExplorer** | • 2.6 build 1083 and later.<br>Some FortiGate models may be supported on specific FortiExplorer versions. |
| **FortiExplorer iOS** | • 1.0.6 build 0130 and later<br>Some FortiGate models may be supported on specific FortiExplorer iOS versions. |
| **FortiExtender** | • 2.0.2 build 0011 and later |
| **AV Engine** | • 5.00227 |
| **IPS Engine** | • 3.00156 |
| **Virtualization Environments** | |
| **Citrix** | • XenServer version 5.6 Service Pack 2<br>• XenServer version 6.0 and later |
| **Linux KVM** | • RHEL 7.1/Ubuntu 12.04 and later<br>• CentOS 6.4 (qemu 0.12.1) and later |
| **Microsoft** | • Hyper-V Server 2008 R2, 2012, and 2012 R2 |
| **Open Source** | • XenServer version 3.4.3<br>• XenServer version 4.1 and later |
| **VMware** | • ESX versions 4.0 and 4.1<br>• ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5 and 6.0 |

FortiGate-VM v5.4 for VMware ESXi (all models), no longer supports the VMXNET2 vNIC driver.

# Language support

The following table lists language support information.

**Language support**

| Language | GUI |
|---|---|
| English | ✔ |
| Chinese (Simplified) | ✔ |
| Chinese (Traditional) | ✔ |
| French | ✔ |
| Japanese | ✔ |
| Korean | ✔ |
| Portuguese (Brazil) | ✔ |
| Spanish (Spain) | ✔ |

# SSL VPN support

## SSL VPN standalone client

The following table lists SSL VPN tunnel client standalone installer for the following operating systems.

**Operating system and installers**

| Operating System | Installer |
|---|---|
| Microsoft Windows XP SP3 (32-bit)<br>Microsoft Windows 7 (32-bit & 64-bit)<br>Microsoft Windows 8 (32-bit & 64-bit)<br>Microsoft Windows 8.1 (32-bit & 64-bit) | 2323 |

| Operating System | Installer |
|---|---|
| Microsoft Windows 10 (32 bit & 64 bit) | 2329 |
| Linux CentOS 6.5 (32-bit & 64-bit)<br>Linux Ubuntu 12.0.4 (32-bit & 64-bit) | 2323 |
| Virtual Desktop for Microsoft Windows 7 SP1 (32-bit) | 2323 |

Other operating systems may function correctly, but are not supported by Fortinet.

## SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

**Supported operating systems and web browsers**

| Operating System | Web Browser |
|---|---|
| Microsoft Windows 7 SP1 (32-bit/64-bit) | Microsoft Internet Explorer version 11<br>Mozilla Firefox version 42 |
| Microsoft Windows 8/8.1 (32-bit/64-bit) | Microsoft Internet Explorer version 11<br>Mozilla Firefox 42 |
| Mac OS 10.9 | Safari 7 |
| Linux CentOS version 6.5 | Mozilla Firefox 42 |

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

## SSL VPN host compatibility list

The following table lists the antivirus and firewall client software packages that are supported.

**Supported Microsoft Windows XP antivirus and firewall software**

| Product | Antivirus | Firewall |
|---|---|---|
| Symantec Endpoint Protection 11 | ✔ | ✔ |
| Kaspersky Antivirus 2009 | ✔ | |
| McAfee Security Center 8.1 | ✔ | ✔ |
| Trend Micro Internet Security Pro | ✔ | ✔ |
| F-Secure Internet Security 2009 | ✔ | ✔ |

**Supported Microsoft Windows 7 32-bit antivirus and firewall software**

| Product | Antivirus | Firewall |
|---|---|---|
| CA Internet Security Suite Plus Software | ✔ | ✔ |
| AVG Internet Security 2011 | | |
| F-Secure Internet Security 2011 | ✔ | ✔ |
| Kaspersky Internet Security 2011 | ✔ | ✔ |
| McAfee Internet Security 2011 | ✔ | ✔ |
| Norton 360™ Version 4.0 | ✔ | ✔ |
| Norton™ Internet Security 2011 | ✔ | ✔ |
| Panda Internet Security 2011 | ✔ | ✔ |
| Sophos Security Suite | ✔ | ✔ |
| Trend Micro Titanium Internet Security | ✔ | ✔ |
| ZoneAlarm Security Suite | ✔ | ✔ |
| Symantec Endpoint Protection Small Business Edition 12.0 | ✔ | ✔ |

# Resolved Issues

The following issues have been fixed in version 5.4.0. For inquires about a particular bug, please contact Customer Service & Support.

**Device Visibility**

| Bug ID | Description |
|---|---|
| 300577 | Add QUIC support in passive device detection. |
| 299500 | Ensure Mac is not detected as an iPhone. |

**DLP**

| Bug ID | Description |
|---|---|
| 282782 | DLP does not stop processing filter(s) after the first match. Therefore, DLP file patterns matching `*.xap` for Silverlight keeps being blocked as an executable. |
| 299924 | Support integration of tag `%%SUBJECT%%` as part of the custom replacement message is set as the email subject. |
| 298236 | Improve credit card number check handled by DLP sensor. |

**Firewall**

| Bug ID | Description |
|---|---|
| 277238 | RSSO set the endpoint `DB record &quot;block status&quot;` to the incorrect value |
| 295643 | Improved authentication daemon optimization. |
| 282807 | NP4lite leaks some `unNATed` packets on the external interface when NAT ports are exhausted. |
| 297421 | HTTPs traffici is blocked after an AV/IPS database update from FortiGuard. |
| 296931 | TCP Window size overruns in FGT when remote server announces the Window Scaling is `0`. |
| 295164 | `oversize-log disable` does not work for FTP downloads. |
| 298411 | When installing `vip` to the kernel, check if the sock list is empty or not when deleting sock list elements. |

| Bug ID | Description |
|---|---|
| 293132, 291689 | Do not offer abbreviated TLS handshake on mismatched versions. |
| 298937 | `Proxyd ssl-exempt` must not check the IP address if a hostname exists. |

### GUI

| Bug ID | Description |
|---|---|
| 258101 | When testing a RADIUS server and it does not connect, an error occurs. |
| 274256 | HTTP 500 error occurs when trying to view a CA certificate. |
| 262009 | GUI shows incorrect IP address and interface for DDNS domains. |
| 275377 | Secondary IP and netmask for VLAN interfaces are reversed. |
| 251641 | *Insert policy below/above* does not work in a multicast policy list. |
| 269191 | Client monitor page is not showing clients when filter is set on SSIDs. |
| 276756 | *Profile groups* > *Ref. links* do not work. |
| 274256 | HTTP 500 error occurs when trying to view a CA certificate. |
| 269191 | Client monitor page is not showing clients when filter is set on SSID. |
| 286110 | GUI shows different certificate name under the VPN SSL setting compared to the CLI. |
| 260886 | Policy dialog cannot load large number of addresses (10,000 or more). |
| 286533 | GUI RADIUS Test Connectivity does not respond to `use-management-vdom set`. |
| 294403 | Users cannot choose or change the Source Device Type in GUI on the SSLVPN Firewall policy. |
| 274588 | Dashboard Status screen incorrectly shows FortiToken status. |
| 272420 | One invisible group is selected in LDAP Remote Group. |

### High Availability

| Bug ID | Description |
|---|---|
| 294950 | `Radiusd` is not able to synch with a database with a secondary unit, the keeps the database locked and prevents users from being able to authenticate. |

| Bug ID | Description |
|---|---|
| 299848 | Remote+Wildcard admin are only matched compared to one group on the slave device. |
| 298647 | `npu_vlinks` receives the same `virtual-mac` in a HA configuration. |
| 283697 | When a new device joins, the list of devices may not synchronize between master and slave. |

### IPS

| Bug ID | Description |
|---|---|
| 260302<br>283644<br>287743 | IPS engine daemon does not rely on the View ID to obtain configuration. |

### IPsec

| Bug ID | Description |
|---|---|
| 294697 | IPsec traffic is blocked after a HA failover. |
| 279519 | When adding and/or modifying a Firewall policy, IPsec traffic stops during a `vlink` and/or `lpck` offload session. |
| 274252 | IPSec VPN phase1 interface does not negotiate SA with its peer when 3G interface comes up. |

### Log & Report

| Bug ID | Description |
|---|---|
| 300881 | Modify service and `log desc` when traffic is denied due to an explicit proxy policy |
| 295179 | Offset the device time field in the logs on the FortiAnalyzer. |

### Routing

| Bug ID | Description |
|---|---|
| 298214 | If two out of four GWs for policy routes go down, one `proute` may be down but another `proute` is incorrectly up. |
| 282126 | `OSPF` should be able to filter incoming external routes by route-map. |
| 296921 | `nssa-default-information-originate` to make a `OSPF` always sends a default route of information to NSSA. |

| Bug ID | Description |
|---|---|
| 298290 | `pim-dm` should use kernel route to query the nexthop, instead of using the NSM module. |
| 299593 | `rip` and `ripng`'s `offset-list` status to be enabled by default. |

### SSLVPN

| Bug ID | Description |
|---|---|
| 297315 | User node cannot be found when the password has changed. |
| 257689 | SSLVPN OWA 2013 send button does not work as expected. |
| 300748 | MS RemoteApp and Desktop Connections are not shown via SSLVPN webportal. |

### SSO

| Bug ID | Description |
|---|---|
| 290746 | FortiGate removes FSSO logins as soon as the Collector agent is disconnected. |

### System

| Bug ID | Description |
|---|---|
| 276628 | `npu-vlink` stops working when adding a transparent VDOM. |
| 295794 | Hardware-switch does not block an access from undefined hosts in the IP/MAC binding table after reboot. |
| 297132 | Kernel and NP6 shaper interprets `set maximum-bandwidth 0` differently. |
| 295022 | Load all CAs in current VDOMs for OCSP certificate verification. |
| 271239 | Admin password authentication cannot be disabled with public key authentication. |
| 301887 | Enable `NPU SynProxy` support for FG-3700DX and FG-5001D. |
| 298828 | Unable to set 31-bit mask for a secondary IP address. |
| 298057 | Root Dispersion and Root Delay of `diagnose sys ntp status` command is an invalid value. |
| 257176 | CPU increases when adding FAPs to FGT-60C-PoE. |
| 301244 | Incoming PPPoE frame is accepted even when the destination MAC address is not local. |

| Bug ID | Description |
|---|---|
| 298867 | GMT +13:00 Samoa time zone with DST is not supported. |
| 297451 | Member port is removed from a software-switch after rebooting if a `management-vdom` is in TP-mode. |
| 297666 | Support CRL download over `HTTP/1.1`. |
| 286771 | `set macaddr` option does not work for a switch-interface. |
| 299585 | Always recycle the `nturbo/ips` local `mbuf` even if the `nturbo` buffer has been removed to avoid a `nturbo mbuf` leak in IPS. |
| 282472 | NP6 Multicast traffic is duplicated. |
| 297478 | `snifferd` process locks administrators even after `admintimeout`. |
| 298204 | FWF-30E/50E/51E goes into the system conserve mode. |
| 276941 | No value is returned when accessing Virtual Switch interface's OIDs. |
| 273124 | Some of the Current Usage information under *VDOM* > *Global Resources* is incorrect. |

### Upgrade

| Bug ID | Description |
|---|---|
| 298540<br>297001 | After HA cluster upgrade, Master and Slave boxes have different checksums for the web-filter profile in the root VDOM. |

### WANopt & Webproxy

| Bug ID | Description |
|---|---|
| 297486 | DNS improvements to handle `fwd proxy server`. |

### WiFi

| Bug ID | Description |
|---|---|
| 265950 | Wifi user unable to access internal applications after enabling Application Control. |
| 240602 | Anonymous identity should not replace the real authentication account when a client is connecting to WPA-Enterprise. |

# Known Issues

The following issues have been identified in version 5.4.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

**Firewall**

| Bug ID | Description |
|---|---|
| 304317, 304136 | `WAD daemon` may crash when enabling `WAD debug`. |
| 304449 | TELNET may not be able to trigger authentication when the application profile and the user group are both configured. |
| 304432 | Protect server may not work as expected when enabling the Proxy AV and deep inspection. |

**FortiGate-VM**

| Bug ID | Description |
|---|---|
| 304802 | Users may lose access to the HTTPS GUI access after upgrading from 5.2.5 due to the `Fortinet_Firmware` certificate being removed.<br><br>**Work around**: `set admin-server-cert` to `Fortinet_Factory` under the `config system global setting`. |

**FortiView**

| Bug ID | Description |
|---|---|
| 303747 | Source > Filter *Source Device* may not work. |
| 289376 | Applying the filter *All* by using the right click method may not work in the All Session page. |
| 301315 | Device Topology page, should add dependency warning if no interface has device detection enabled. |
| 303940 | Web Site > Security Action filter may not work |
| 277558 | Policy page > IPv6 policy may be displayed as IPv4 policy in realtime view. |
| 303787 | Application page > Filter on a Unknown Application may not work. |
| 303823 | Policy page > Source and Destination interface might show `unknown-0` message. |

| Bug ID | Description |
|---|---|
| 300055 | In Traffic Shaping page , bandwidth and dropped bytes may not be accurately listed for the Forward Shaper. |
| 299900 | In the Traffic shaping page, the IPv6 shaping may miss `reply-shaper name` and may not be able to drill down the menu. |

**GUI**

| Bug ID | Description |
|---|---|
| 289297 | Threat map may not be fully displayed when screen resolution is not big enough. |
| 302633 | Several list pages may have alignment issues with Chrome 47. |
| 303928 | After upgrading from 5.2 to 5.4, the default flow based AV profile may not be visible or selectable in the Firewall policy page in GUI. |
| 303642 | Route lookup window may be empty. |
| 303645 | If no route is found, the IPv6 route lookup result may not be accurate. |
| 302576 | GUI may display the `password-policy` rules on the Admin page even the `password-policy` does not apply to that admin user. |
| 303038 | Dead Peer Detection setting in IPsec tunnel templates page may show *on-demand* instead of *enable*. |
| 303776 | There may not be any options available in the Log View; a JS error occurs when setting a filter in the protocol field. |
| 304100 | Users may not be able to enable Feature Select in Global or VDOM on the following platforms: FG-3700D, FG-3700DX, FG-3810D and FG-5001D. |
| 304119 | Explicit Proxy Policy may receive an internal error if *All Ports* is enabled in any of `ssl-ssh` certificates in the inspection profile. |
| 304482 | NP6 offloading may be lost when the IPsec interface has the `aes256gcm` proposal. |
| 304491 | Users may not be able to set the *IPsec VPN Xauth User Group* to *inherit groups from policy* in GUI. |
| 304495 | In *Network* > *Explicit Proxy* page, when users edit *Listen on Interfaces*, the page may stop responding. |
| 304395 | The SSLVPN Web Portal RSA token in New Pin Mode may notwork. |
| 304645 | Traffic Shapers bandwidth unit may display kb/s while the backend config has mbps/gbps. |

| Bug ID | Description |
|---|---|
| 304627 | In the HA setup, restoring config in GUI, only master's config might be restored, but slave's config may not be restored. |
| 304436 | GUI might show a different received/sent value with CLI on *GUI->Modem* monitor page. |
| 304439 | Users may not be able to set UTM profiles in IPsec Action Policy page. |
| 304455 | *GUI > Interface > DHCP Server > Advanced > DHCP Client List* page may not display correctly on Chrome 47. |

### High Availability

| Bug ID | Description |
|---|---|
| 304433 | New import local certificate may cause the HA to become out of sync in a multi VDOM environment.<br><br>**Workaround**: reboot the master. |

### IPS

| Bug ID | Description |
|---|---|
| 306277 | Flowed base local url filter may not work on FGT-3700D/FGT-1500D. |

### IPsec

| Bug ID | Description |
|---|---|
| 296439 | `L2TP over IPsec tunnel` may not be able to be established. |

### Log & Report

| Bug ID | Description |
|---|---|
| 304217 | `miglogd` may stop working its protocol and port overlap is with another service.<br><br>**Affected policy**: IPv4/IPv6 multicast policy, IPv4/IPv6 DOS policy and sniffer policy. |
| 304533 | AntiVirus log may not have a URL section when a Gmail attachment is downloaded. |

### SSLVPN

| Bug ID | Description |
|---|---|
| 282914 | If users use SSLVPN in Web Mode, they may not be able to access a FortiGate running 5.4. |
| 300054 | SSLVPN login replacement messages may be reset to factory default when upgrading from 5.2. |
| 304528 | SSLVPN Web Mode PKI user might immediately log back in even when logging out. |
| 304139 | SSLVPN *Login Anyway* might not work when `limit-user-logins` is enabled. |
| 303661 | The *Start Tunnel* feature may have been removed. |

### System

| Bug ID | Description |
|---|---|
| 275631 | Multicast traffic may be able to be offloaded by XLP in NAT mode when there is no PIM enabled. |
| 295292 | If `private-data-encryption` is enabled, when restoring config to a FortiGate, the FortiGate may not prompt the user to enter the key. |
| 301947 | On NP6 ports, `hairpinned` traffic may be blocked after the traffic that initializes the original NATs stops responding.<br>**Workaround**: disable `fastpath` on the NP6 port. |
| 303626 | Switch VLAN may not be accessible in trunk (LACP) mode on 200 series platforms. |
| 297923 | Newly created HW switch on NP4 platforms may not be accessible until users reboot. |
| 290708 | `nturbo` may not support CAPWAP traffic. |
| 304118 | VLAN and hardware switch interface may lose the secondary IP during the upgrade from v5.2 to v5.4.<br><br>**Workaround**: `unset role under config system interface` then manually adding the secondary IP back. |
| 303906 | The CLI may stop working when configuring Interface Policy6. |
| 298348 | IPv6 may not work on the internal interface.<br><br>**Affected platform**: FGT-92D |
| 304472 | `Health-check over pppoe` interface may not work after a FGT reboot. |

| Bug ID | Description |
|---|---|
| 304320 | LENC FGT may not be able to update the `modem-list` and `message-update`; it may not be able to connect to FortiAnalyzer. |
| 303959 | When the VDOM is enabled, the `EAP_proxy` may not be able to handle the certificate chain with a depth of more than two. |
| 304667 | When FGT has only one disk and it is used by WANopt, the factory reset may not reset the disk to log.<br><br>**Workaround**: use CLI to `set disk-usage to log` under `config system global`. |
| 305058 | FortiGate may encounter a system hang issue caused by the `dialup ipsec vpn`. The `unregister_netdevice` error message may appear. |

### Upgrade

| Bug ID | Description |
|---|---|
| 269799 | `sniffer config` may be lost after upgrade. |
| 289491 | When upgrading from 5.2.x to 5.4.0, `port-pair` configuration may be lost if the `port-pair` name exceeds 12 characters. |
| 273973 | When upgrading from 5.2 to 5.4, the Central NAT feature cannot be upgraded. After the upgrade, reconfigure the Central NAT feature. Please see the configuration examples in the FortiOS Handbook available in the Fortinet Document Library. |

### WANopt & Webproxy

| Bug ID | Description |
|---|---|
| 291241 | WAD may have a `fd leak` after concurrent tests. |
| 271526 | A WAD session leak may occur. |

# Limitations

## Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

## Open Source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.

FORTINET®

*High Performance Network Security*